

## Multiple Examples of DSA

FIPS 186-2 with Change Notice #1 dated October 5, 2001 allows the PRNG to be either the one originally specified in Appendix 3 of the standard or the one specified in the Change Notice. Additionally, these PRNG's specify the use of a one-way function  $G(t,c)$ . These examples include both the original and Change Notice versions of the PRNG's, as well two different  $G(t,c)$  functions (the first is based on SHA-1 and the second is based on DES).

### 1. 1024-bit Modulus with Original PRNG, $G(t,c)$ using SHA-1

The following SEED value is from step 1 on Appendix 2.2:

SEED= 1444c1df 2830a665 9a80ed71 c06e9de5 0652f7ea

And results in the following values for  $q$  and  $p$ :

q= b5afdf2f9 3246b1ef cd1f3a7c 240c1e9e 21a3630b  
p= a65feaab 511c61e3 3df38fdd daf03b59 b6f25e1f  
a4de57e5 cf00ae47 8a855dda 4f3638d3 8bb00ac4  
af7d8414 c3fb36e0 4fbdf3d3 166712d4 3b421bfa  
757e8569 4ad27c48 f396d03c 8bce8da5 8db5b820  
39f35dcf 857235c2 f1c73b22 26a36142 9190dcb5  
b6cd0edf b0ff6933 900b02ce cc0ce692 74d8dae7  
c6948043 18d6d6b9

With the following counter value:

counter= 24

To compute the value of  $g$  using the method in Appendix 4 (not a requirement of the standard), the following value of  $h$  was selected in step 3:

h= 2

And produces:

g= 007bbd2c 5dc917a5 e08b9c2f 80a49fb6 3fcfd5c05  
78ba701e 254fe353 0dedd3b6 680a6e5a fb3280b5  
3f154028 bafff73d 1ba0fdb0 004b9eb0 dbf24b29  
5bf2a356 913cd1c0 be03c510 3a1da8b7 3e7670b5  
6d716ed5 547af67b 5061311e ea245e2e 5c337843  
cbc135b9 b9c18775 d5d56cf9 a31b747e 2449861a  
df3b3f72 7189c0a3

Using the algorithm in Appendix 3.1 for the generation of  $x$  values:

```
XKEY=      bd029bbe 7f51960b cf9edb2b 61f06f0f eb5a38b6  
XSEED=     00000000 00000000 00000000 00000000 00000000  
XVAL=      bd029bbe 7f51960b cf9edb2b 61f06f0f eb5a38b6
```

Using the routine in Appendix 3.3 Constructing The Function G From SHA-1 provides:

```
x=      2070b322 3dba372f de1c0ffc 7b2e3b49 8b260614
```

The following value is the updated XKEY value from step 3.d:

```
XKEY=      dd734ee0 bd0bcd3b adbaeb27 dd1eaa59 76803ecb
```

The value of  $x$  computed above results in the following  $y$  value:

```
y=      87c9b20a aef34afc bd6ffb55 09e7cb3b 43f8bec5  
6ba74ad0 89d2ac26 59b9fa8f 895d51b5 9891f0a5  
afe8b2e1 1ae133ac 16529fffc 031eedf7 834f6c1b  
ce2604c4 e5cc750d f577d29c 08f0a6e4 f7e190d2  
1b683fb6 e08f4d9e a6ea1f03 d7720cea 0a97c039  
69118dea 97d3efc3 0d0dc80 495cf2ea 84eac1b4  
4fb3d2b8 e25e0bd8
```

  

```
M=      ASCII form of "abc"
```

  

```
SHA-1(M)= a9993e36 4706816a ba3e2571 7850c26c 9cd0d89d
```

Using the algorithm in Appendix 3.2 for generation of  $k$  values:

```
KKEY=      687a66d9 0648f993 867e121f 4ddf9ddb 01205584
```

Using the routine in Appendix 3.3 Constructing The Function G From SHA-1 provides:

```
k=      4750fbea 559a880e 1cfe6980 e35c411c 97d60e13
```

The following value is the updated KKEY value from step 3.d:

```
KKEY=      afcb62c3 5be381a1 a37c7ba0 313bdef7 98f66398
```

The method in Appendix 4 provides the following value of  $k^{-1}$ :

```
k-1=      74884c0c 2bccf6c1 f2f225e8 cb5352e9 b5590aa5
```

Computing the Digital Signature as specified in Section 5:

```
r= b1d237b1 af083174 9cfa5557 edf2327b 84835270  
s= 1711e4c0 94cf31a 33b2fc71 e8cc7061 7b31ab52
```

Verifying the Digital Signature as specified in Section 6:

```
w= 01f8f24c c5249634 db93f9b0 ab2ecacd 63868502  
u1= 49db8fa7 93c1726f 025b6354 6094927b 55b1fb89  
u2= 3a05c13e 9f9a9dc7 b5525be4 84574fa4 535588bb  
gu1 mod p= 77bb0678 dd781c4e 95b43893 26d43749 f6604981  
41e56695 c724c06b 96f2e15c 3bfe605b eaf55c7e  
7f42b0b5 9696da5f 2ee65cb8 c83b2f19 2bad08b1  
814be325 36c4b819 8b04c2c0 019d5a79 eb7cbf9d  
6f47b063 a1bbca1f 39a2212f a3f4b4b5 261dc041  
43ea563c cfcc1504 a6cd6ac1 08fcc407 fff6c0ae  
c6091c90 49e40b4b  
yu2 mod p= 8799225f d0943d2e c39d25f8 f10e737e c0ef0c6b  
9c9574a7 37f48aa2 90417c87 5bcce77f 7a472b8a  
d8c4fb7d 1d7cb990 3f2524e1 f710acce 3f868ff7  
2a580e38 ce04434c a95e22de 74770119 1355f063  
14a5dbf5 4ce25d8b 0208b515 12acb9e9 bb818924  
ddd86e84 7e100c98 012466a2 4084c5f0 616bb574  
1a8ebf80 7bc71887  
v= b1d237b1 af083174 9cfa5557 edf2327b 84835270
```

Since  $v=r'$ , the signature is verified.

## 2. 1024-bit Modulus with Change Notice PRNG, G(t,c) using SHA-1

The following SEED value is from step 1 on Appendix 2.2:

```
SEED= 1444c1df 2830a665 9a80ed71 c06e9de5 0652f7ea
```

And results in the following values for  $q$  and  $p$ :

```
q= b5afdf2f9 3246b1ef cd1f3a7c 240c1e9e 21a3630b  
p= a65feaab 511c61e3 3df38fdd daf03b59 b6f25e1f  
a4de57e5 cf00ae47 8a855dda 4f3638d3 8bb00ac4
```

```

af7d8414 c3fb36e0 4fbdf3d3 166712d4 3b421bfa
757e8569 4ad27c48 f396d03c 8bce8da5 8db5b820
39f35dcf 857235c2 f1c73b22 26a36142 9190dcb5
b6cd0edf b0ff6933 900b02ce cc0ce692 74d8dae7
c6948043 18d6d6b9

```

With the following counter value:

```
counter= 24
```

To compute the value of  $g$  using the method in Appendix 4 (not a requirement of the standard), the following value of  $h$  was selected in step 3:

```
h= 2
```

And produces:

```

g= 007bbd2c 5dc917a5 e08b9c2f 80a49fb6 3fcfd5c05
78ba701e 254fe353 0dedd3b6 680a6e5a fb3280b5
3f154028 baafff73d 1ba0fdb0 004b9eb0 dbf24b29
5bf2a356 913cd1c0 be03c510 3a1da8b7 3e7670b5
6d716ed5 547af67b 5061311e ea245e2e 5c337843
cbc135b9 b9c18775 d5d56cf9 a31b747e 2449861a
df3b3f72 7189c0a3

```

Using the revised algorithm found in the Change Notice for the generation of  $x$  values:

```
XKEY= bd029bbe 7f51960b cf9edb2b 61f06f0f eb5a38b6
```

```
XSEED= 00000000 00000000 00000000 00000000 00000000
```

The first loop through step 3.2 provides:

```
XVAL= bd029bbe 7f51960b cf9edb2b 61f06f0f eb5a38b6
```

Using the routine in Appendix 3.3 Constructing The Function G From SHA-1 provides:

```
w[ 0 ]= 2070b322 3dba372f de1c0ffc 7b2e3b49 8b260614
```

The following value is the updated XKEY value from step 3.2.c:

```
XKEY= dd734ee0 bd0bcd3b adbaeb27 dd1eaa59 76803ecb
```

The second loop through step 3.2 provides:

```
XVAL= dd734ee0 bd0bcd3b adbaeb27 dd1eaa59 76803ecb
```

Using the routine in Appendix 3.3 Constructing The Function G From SHA-1 provides:

w[1] = 3c6c18ba cb0f6c55 babb1378 8e20d737 a3275116

The following value is the updated XKEY value from step 3.2.c:

XKEY= 19df679b 881b3991 6875fea0 6b3f8191 19a78fe2

Step 3.3 provides the following values:

w[0] || w[1] = 2070b322 3dba372f de1c0ffc 7b2e3b49 8b260614  
3c6c18ba cb0f6c55 babb1378 8e20d737 a3275116

X= 47c27eb6 16dba413 91e5165b e9c5e397 7e39a15d

The value of X computed above results in the following y value:

y= 6f072da4 e8787a82 d1a37e23 ac7f843f 4f3696b1  
92f4f062 f3687084 a3185669 8dea64bd 3710e151  
64b52a33 e6a6080f c5b00596 ddbc0bc1 aa4aabaa3  
61666dee efba6a93 cb99c9fb 37e3c2a2 4b20922a  
7add1dd4 d5cf23a6 9d6a285a 27d18ed0 824ae59c  
7a8228ac c259e5f7 f10d163f 08858dee b897c22b  
9abb4282 16e51c47

M= ASCII form of "abc"

SHA-1(M)= a9993e36 4706816a ba3e2571 7850c26c 9cd0d89d

Using the revised algorithm found in the Change Notice for the generation of k values:

KKEY= 687a66d9 0648f993 867e121f 4ddf9ddb 01205584

The first loop through step 3.1 provides:

Using the routine in Appendix 3.3 Constructing The Function G From SHA-1 provides:

w[0] = fd00cee3 87e139fd ea1da3fd 07685fba b979711e

The following value is the updated KKEY value from step 3.1.b:

KKEY= 657b35bc 8e2a3391 709bb61c 5547fd95 ba99c6a3

The second loop through step 3.1 provides:

Using the routine in Appendix 3.3 Constructing The Function G From SHA-1 provides:

w[1] = bfb1c43b a8c9326c 16d8a3aa a3e35b30 b4349b31

The following value is the updated KKEY value from step 3.1.b:

XKEY= 252cf9f8 36f365fd 877459c6 f92b58c6 6ece61d5

Step 3.2 provides the following values:

w[0] || w[1] = fd00cee3 87e139fd e1da3fd 07685fba b979711e  
bf1c43b a8c9326c 16d8a3aa a3e35b30 b4349b31

k= 952127c8 c4b38b8b ffb0defa 5ff6af91 a2a81296

The method in Appendix 4 provides the following value of  $k^{-1}$ :

$k^{-1}$  = 088388e1 34d2da64 3c54844b 0febe082 c196e815

Computing the Digital Signature as specified in Section 5:

r= 6b4fbb0 98a514a2 3bb89c67 0587bc0d aaelfa69

s= 84737cc0 7b3ef5f6 2806c4c5 87d9e97f 2dfac5cc

Verifying the Digital Signature as specified in Section 6:

w= 03512709 097081db d023d9bb 63a25808 b345e7bc

u1= 86d68eba 67a36c27 0dc74cab 64f7b37f fce29071

u2= 6c332119 44b43db8 3589d044 a66ab573 58b2b305

$g^{u1} \bmod p$  = 73394ea6 ebbfbceb 81c3b466 786aacfb 27f1187b  
5e37905d 6526c793 11d9c6ce 40a0515a b7cc882e  
9134d050 f0c0ea79 a3ab3dfa a9daabff 0531bbdf  
d1f92482 edbfa8d5 907b5678 61f24386 ee785b69  
3786f01e 9a7b1ce3 693bdf56 31df92bb 0b644b4d  
acaf8ffc 9b141690 e82cb51d 46af6747 0b848e4b  
2db2e8bc 13362f9f

$y^{u2} \bmod p$  = 6f4433be 3c89f6a7 ec02d08b d495ca51 5c91159a  
cb962035 8ab3e48a 97aebb7e 733660c7 0128ba8c  
00ec5365 46d9f9d2 1373f259 346600fe b59f239f  
1dbc25ed 82b58430 e9980570 193dd8e9 299fe62a

```

0b867392 b1979bfe aae916a9 0b7e8906 e7177eb4
d2ef78c7 395c4a8f 68334a7e f5735f34 13fb5be8
79016955 97c3a799

v=      6b4fbcbc0 98a514a2 3bb89c67 0587bcfd aaelfa69

```

Since  $v=r'$ , the signature is verified.

### 3. 1024-bit Modulus with Original PRNG, G(t,c) using DES

The following SEED value is from step 1 on Appendix 2.2:

```
SEED= 1444c1df 2830a665 9a80ed71 c06e9de5 0652f7ea
```

And results in the following values for  $q$  and  $p$ :

```

q=      b5af2f9 3246b1ef cd1f3a7c 240c1e9e 21a3630b

p=      a65feaab 511c61e3 3df38fdd daf03b59 b6f25e1f
       a4de57e5 cf00ae47 8a855dda 4f3638d3 8bb00ac4
       af7d8414 c3fb36e0 4fbdf3d3 166712d4 3b421bfa
       757e8569 4ad27c48 f396d03c 8bce8da5 8db5b820
       39f35dcf 857235c2 f1c73b22 26a36142 9190dc5
       b6cd0edf b0ff6933 900b02ce cc0ce692 74d8dae7
       c6948043 18d6d6b9

```

With the following counter value:

```
counter= 24
```

To compute the value of  $g$  using the method in Appendix 4 (not a requirement of the standard), the following value of  $h$  was selected in step 3:

```
h= 2
```

And produces:

```

g=      007bbd2c 5dc917a5 e08b9c2f 80a49fb6 3fcfd5c05
       78ba701e 254fe353 0dedd3b6 680a6e5a fb3280b5
       3f154028 baaff73d 1ba0fdb0 004b9eb0 dbf24b29
       5bf2a356 913cd1c0 be03c510 3a1da8b7 3e7670b5
       6d716ed5 547af67b 5061311e ea245e2e 5c337843
       cbc135b9 b9c18775 d5d56cf9 a31b747e 2449861a
       df3b3f72 7189c0a3

```

Using the algorithm in Appendix 3.1 for the generation of  $x$  values:

```

XKEY=      bd029bbe 7f51960b cf9edb2b 61f06f0f eb5a38b6
XSEED=     00000000 00000000 00000000 00000000 00000000
XVAL=      bd029bbe 7f51960b cf9edb2b 61f06f0f eb5a38b6

```

Using the routine in Appendix 3.3 Constructing The Function G From DES provides:

```
x=      33db34a8 93e76615 f2f5e399 599db156 8aa89d7b
```

The following value is the updated XKEY value from step 3.d:

```
XKEY=      f0ddd067 1338fc21 c294bec4 bb8e2066 7602d632
```

The value of  $x$  computed above results in the following  $y$  value:

```

y=      009c5efb 451cb8fa 3a0b925b 02917b05 899c4787
       33b017de d4302467 ef88ff77 080cd5d9 21603d2b
       b9ad8861 2244b03e ede94596 dbed2ddc ab44bed3
       a4dd34f5 28adb246 a4075eac 883066a7 22739017
       2ebfb601 dd8706e5 2fb487e1 38069dc4 3fe99492
       064f3225 b57ec688 5a8cb3c1 26d18575 9ac83d5b
       997f52c0 56394f3e

```

```
M=      ASCII form of "abc"
```

```
SHA-1(M)= a9993e36 4706816a ba3e2571 7850c26c 9cd0d89d
```

Using the algorithm in Appendix 3.2 for generation of  $k$  values:

```
KKEY=      687a66d9 0648f993 867e121f 4ddf9ddb 01205584
```

Using the routine in Appendix 3.3 Constructing The Function G From DES provides:

```
k=      1b053e51 4ed015ea 83df13cd 5ee31d61 1598030e
```

The following value is the updated KKEY value from step 3.d:

```
KKEY=      837fa52a 55190f7e 0a5d25ec acc2bb3c 16b85893
```

The method in Appendix 4 provides the following value of  $k^{-1}$ :

```
 $k^{-1}$ =      7ae9c451 cddf8f00 60fe8db1 ff46ae8c ec3ddaa
```

Computing the Digital Signature as specified in Section 5:

```

r=      71e91955 9a3945b3 603cda57 da315734 762f2dc3
s=      2a55c855 833a776b 395f5d04 7c4a6529 c7ca51ea

```

Verifying the Digital Signature as specified in Section 6:

```

w=      6ced295e 3a1c8dae fb6b58c3 c20ee326 c03b36cc
u1=     9581eefaa 3df8a0e7 03487c80 8197c9a5 90ccb2c1
u2=     93adb420 4ebale41 c4616fca 1c6d96c1 162e7220
gu1 mod p= 5dcaebcd 4746095d 1598b7f1 f23458e2 2b0d706f
             1623042c 20240fde b4a06130 4f985d36 73af0230
             5b106ff6 0fc60aa4 a89b20e9 5ab7bb55 f60be18f
             5a8151b8 8d9f3f55 dbf2f420 68d09e3c 9cbf639a
             c800833e 6b61135e 78edc7a8 416db585 493591ba
             1087b699 05e5fd0b 5a7dedbc 36e7ac89 7e9c269b
             7018565e 8cecccc28

yu2 mod p= 458cfb37 fa1ddbf3 23c40661 db7f8078 c2cd297b
             f582efb5 cc685648 f5404dba 71dff006 87776ee3
             00bf75ba 1bfb7ddb e4e43a23 8195f330 c7546d13
             81543b10 3de32feb 586a6e86 7cea59b3 444d7944
             1d4ae1c9 ed202316 73cd1624 c00dfe86 bc774221
             4793131a a1637909 473f81fd c7094a4c 4bec8660
             f3e8ccda 5014bf6c

v=      71e91955 9a3945b3 603cda57 da315734 762f2dc3

```

Since  $v=r'$ , the signature is verified.

#### 4. 1024-bit Modulus with Change Notice PRNG, G(t,c) using DES

The following SEED value is from step 1 on Appendix 2.2:

```
SEED= 1444c1df 2830a665 9a80ed71 c06e9de5 0652f7ea
```

And results in the following values for  $q$  and  $p$ :

```

q=      b5afdf2f9 3246b1ef cd1f3a7c 240c1e9e 21a3630b
p=      a65feaab 511c61e3 3df38fdd daf03b59 b6f25e1f
             a4de57e5 cf00ae47 8a855dda 4f3638d3 8bb00ac4
             af7d8414 c3fb36e0 4fbdf3d3 166712d4 3b421bfa
             757e8569 4ad27c48 f396d03c 8bce8da5 8db5b820

```

```
39f35dcf 857235c2 f1c73b22 26a36142 9190dcb5  
b6cd0edf b0ff6933 900b02ce cc0ce692 74d8dae7  
c6948043 18d6d6b9
```

With the following counter value:

```
counter= 24
```

To compute the value of  $g$  using the method in Appendix 4 (not a requirement of the standard), the following value of  $h$  was selected in step 3:

```
h= 2
```

And produces:

```
g= 007bbd2c 5dc917a5 e08b9c2f 80a49fb6 3fc5c05  
78ba701e 254fe353 0dedd3b6 680a6e5a fb3280b5  
3f154028 bafff73d 1ba0fdb0 004b9eb0 dbf24b29  
5bf2a356 913cd1c0 be03c510 3a1da8b7 3e7670b5  
6d716ed5 547af67b 5061311e ea245e2e 5c337843  
cbc135b9 b9c18775 d5d56cf9 a31b747e 2449861a  
df3b3f72 7189c0a3
```

Using the revised algorithm found in the Change Notice for the generation of  $x$  values:

```
XKEY= bd029bbe 7f51960b cf9edb2b 61f06f0f eb5a38b6
```

```
XSEED= 00000000 00000000 00000000 00000000 00000000
```

The first loop through step 3.2 provides:

```
XVAL= bd029bbe 7f51960b cf9edb2b 61f06f0f eb5a38b6
```

Using the routine in Appendix 3.3 Constructing The Function G From SHA-1 provides:

```
w[ 0 ]= 33db34a8 93e76615 f2f5e399 599db156 8aa89d7b
```

The following value is the updated XKEY value from step 3.2.c:

```
XKEY= f0ddd067 1338fc21 c294bec4 bb8e2066 7602d632
```

The second loop through step 3.2 provides:

```
XVAL= f0ddd067 1338fc21 c294bec4 bb8e2066 7602d632
```

Using the routine in Appendix 3.3 Constructing The Function G From SHA-1 provides:

w[1] = 0729b5cd 6adfec09 f2094828 51793dae 21b4adc3

The following value is the updated XKEY value from step 3.2.c:

XKEY= f8078634 7e18e82b b49e06ed 0d075e14 97b783f6

Step 3.3 provides the following values:

w[0] || w[1] = 33db34a8 93e76615 f2f5e399 599db156 8aa89d7b  
0729b5cd 6adfec09 f2094828 51793dae 21b4adc3

x= b1f20d51 528ee537 82626cd4 18c527ac bd8f91ea

The value of X computed above results in the following y value:

y= 03d4d023 2bb7d4ba be0303a7 bd78af24 36ad9249  
674e7df e 7b6749e9 115d36be 05ed94b6 02217a27  
c10d12dc 24adf0e8 9ececb6c cf25724a 10beabb2  
a2c72ad3 ae5e03da 40a0ab32 7660b7e5 0eba19e3  
7b722f96 5177d04b 67b86fd3 d9dc5ec7dbe1f858  
046b1c96 e614647f 90525593 6d7cec80 c0eec59c  
63a48d3a c5ef6e26

M= ASCII form of "abc"

SHA-1(M)= a9993e36 4706816a ba3e2571 7850c26c 9cd0d89d

Using the revised algorithm found in the Change Notice for the generation of k values:

KKEY= 687a66d9 0648f993 867e121f 4ddf9ddb 01205584

The first loop through step 3.1 provides:

Using the routine in Appendix 3.3 Constructing The Function G From SHA-1 provides:

w[0] = d0b5114a 8116c7da 50fe4e49 82ef3bff 373b6619

The following value is the updated KKEY value from step 3.1.b:

KKEY= 392f7823 875fc16d d77c6068 d0ced9da 385bbb9e

The second loop through step 3.1 provides:

Using the routine in Appendix 3.3 Constructing The Function G From SHA-1 provides:

w[1] = e3f78fee 775c4911 a1e0d657 46b6c91e 27bc8333

The following value is the updated KKEY value from step 3.1.b:

XKEY= 1d270811 febc0a7f 795d36c0 1785a2f8 60183ed2

Step 3.2 provides the following values:

w[0] || w[1] = d0b5114a 8116c7da 50fe4e49 82ef3bff 373b6619  
e3f78fee 775c4911 a1e0d657 46b6c91e 27bc8333

k= 0364e645 f35eb8fb 3b1f0e07 277f1134 3536e5ba

The method in Appendix 4 provides the following value of  $k^{-1}$ :

$k^{-1}$  = 3a3e83ca 0fa7ed92 0ff68fc9 903cb36b c9195597

Computing the Digital Signature as specified in Section 5:

r= 379222e2 5d61e3bc c7a3b681 b8cb7bab 55280633

s= acb99c8b 80637172 68656314 e770448a 08e5964b

Verifying the Digital Signature as specified in Section 6:

w= 65f61738 eef4a6b9 038fea72 28a515b9 e8fd272a

u1= 63436a18 cc3ba777 f67b7dff a8fcfa94 6511112b

u2= 9628a77a d7001594 96c3a094 837a31d9 c46560a2

$g^{u1} \bmod p$  = 58d2a301 42c4e6b3 07b74df5 8b8204a4 b095d85c  
d55b7aae 5d3b15d0 b5bdb734 92f081a8 864905ce  
e83cd4ee 74c81027 52773fd7 de634e61 80fac555  
84341bc5 ddb7b084 5311d747 28effcc0 87dale85  
0280a2fa 5afdf18b7 bd84a198 9710a44e c85a350e  
eabdale5 2f183691 d393a82f 87c54689 8a72f41c  
6b995428 3cd64197

$y^{u2} \bmod p$  = 355b8438 23749270 d04c0129 f5505f3c b6f53209  
5b66e537 0e49c62e 78360f65 30870474 8bca3f86  
c43e9830 eee6c8cc 01e94b86 b5cae35f 82d767e4  
af9ec1b6 56be0a34 1a42c9b8 97c624c7 32227626  
de554172 7d9f82ff 345df780 6aa71ba7 3cc57dee

b5b7c67a b5be5177 2bff66eb df1d415c a930e627  
a6efefd5 21df9dde

v= 379222e2 5d61e3bc c7a3b681 b8cb7bab 55280633

Since  $v=r'$ , the signature is verified.